iTS Mississippi Department of
Information Technology Services

3771 Eastwood Drive
Jackson, MS 39211-6381
Phone: 601-432-8000
Fax: 601-713-6380
www.its.ms.gov

David C. Johnson, Executive Director

RFP Questions and Clarifications Memorandum

To: Vendors Responding to RFP Number 4246 for the Mississippi Department of Information Technology Services (ITS)

From: David C. Johnson

Date: May 6, 2022

Subject: Responses to Questions Submitted and Clarifications to Specifications

Contact Name: Bill Brinkley

Contact Phone Number: 601-432-8241

Contact E-mail Address: Bill.Brinkley@its.ms.gov

RFP Number 4246 is hereby amended as follows:

1. Title page, INVITATION is modified as follows:

INVITATION: Sealed proposals, subject to the attached conditions, will be received at this office until **May 26 ~~April 21~~, 2022 @ 3:00 p.m.** Central Time for the acquisition of the products/services described below for **Mississippi Department of Information Technology Services.**

2. Title page, third box is modified as follows:

PROPOSAL, SUBMITTED IN RESPONSE TO
RFP NO. 4246
DUE May 26 ~~April 21~~, 2022 @ 3:00 p.m.,
ATTENTION: Bill Brinkley

3. Section VII Technical Specifications, Item 3 Project Schedule is amended as follows:

Task	**Date**
Deadline for Questions Answered and Posted to ITS Web Site	05/06/22 ~~04/08/2022~~
Proposal Due and Open	05/26/22 ~~04/21/2022~~
ITS Board Presentation	07/21/22 ~~06/16/2022~~
Contract Negotiation	August 2022 ~~06/17/2022~~
Proposed Project Implementation Start-up	September 2022 ~~July2022~~

4. Exhibit A Standard Contract, ARTICLE 3, SCOPE OF SERVICES, Item 3.2 H is being modified to read:

H. Notifying ITS a minimum seven (7) days prior to any anticipated service interruption, with said notice containing a general description of the reason for the service interruption;

5. Section VII, Technical Specification, Item 11.3.3 is being modified to read:

11.3.3 The Enterprise State Network currently has a 10Gbps connection to the Internet.

6. Section VII, Technical Specification, Item 11.3.4 is being modified to read:

11.3.4 Utilization of the 10Gbps link averages approximately 40% during business hours, comprised by both client usage and inbound traffic to State servers.

7. Section VII, Functional/Technical Requirements, Item 12.12 is being modified to add:

12.12.8 Blocking based on country/geographic region

8. Section VIII, Cost Submission is hereby replaced with Attachment A, Revised Cost Information Submission.

Vendor must include in their proposal a response to each amended requirement as listed above. Vendor must respond using the same terminology as provided in the original requirements.

The following questions were submitted to ITS and are being presented as they were submitted, except to remove any reference to a specific vendor. This information should assist you in formulating your response.

Question 1: The RFP requires “Will Comply” or “Exception” answers. For items where there is no vendor response required is “Acknowledge” an acceptable answer?

Response: Vendor must respond as indicated in Section VII, Item 1. “Will Comply” or “Exception” are the only permissible responses.

Question 2: Clarification of “legacy malware protection”

Response: “Legacy malware protection” is the ability to detect and block “Signature-based malware” as referenced in Section VII Item 12.12.1.

Question 3: How many users are you going to support with the proposed solution? Are you expecting the cost to relate to this number of users?

Response: The final number of users is unknown, but the State has approximately 27,000 state employees. The State does expect vendors to use this number to determine how they price their individual offerings.

Question 4: Is ITS looking for pricing discounts based on number of units or number of systems deployed statewide?

Response: **The State strives to make the best use of taxpayer dollars and will not turn down additional discounts based on the number of units/systems that are deployed with other entities statewide; however, this type of discounting is not required. Discounts with dependencies will not be used in the evaluation of cost proposals.**

Question 5: Can you specify how much of the “40% of 5Gbps” is user/outbound traffic?

Response: **Section VII Items 11.3.3 and 11.3.4 contained a typographical error. Please see Amendment Numbers 5 and 6 above.**

ITS has a combined 10 Gbps of internet access available for the Enterprise State Network (2 x 5 Gbps geographically diverse redundant circuits). Over the last 30 days, below are the average/min/max during peak business hour usage:

Transmit (from state network destined to internet)

- **Min: 400 Mbps**
- **Max: 2.0 Gbps**
- **Average: 1.4 Gbps**

Receive (from internet to state network)

- **Min: 1.1 Gbps**
- **Max: 3.9 Gbps**
- **Average: 3.1 Gbps**

Question 6: Does the customer want their IPs advertised from the SWG Solution or are they wanting the traffic when leaving and going to the SWG solution to be state-owned IP addresses? Is X-Forwarded-For (XFF) acceptable?

Response: **The State is open to options. Traffic leaving the State’s firewall will be state-owned IP’s. ITS has additional IP’s that we could assign to the SWG solution or would be willing to entertain a X-Forwarded-For option. Regardless of the solution chosen, the State is interested in receiving Netflow/IPFIX data from the SWG solution.**

Question 7: Need information about existing architecture, including high level diagram, edge hardware details (firewall and routers). Is there an existing WCCP solution (what is it handling today)?

Response: **There is no enterprise level WCCP implementation, but individual agencies may use a solution. ITS will provide a detailed diagram in separate email sent to each vendor that attended the mandatory vendor conference.**

Question 8: Is syslog the only method AT&T Threat Manager can ingest logs? What other methods are available?

Response: **Besides syslog, the SIEM also supports API and custom integrations. Either of these offerings may incur professional services charges for setup or customization. Syslog is the State’s preferred method. Over the course of the resulting contract from this RFP, the State could change SIEM**

solutions and expects the Secure Web Gateway vendor to work with the State on future changes.

If a vendor would like to provide future cost associated with this activity, please provide that cost in the Optional Table in the Revised Cost Information Submission.

Question 9: 12.11 The Solution must be able to manage bandwidth at the agency level for upstream and downstream traffic. Is this referring to traffic shaping or rate-limiting? Or reporting on bandwidth used?

Response: This is referring to rate-limiting traffic.

Question 10: 12.12.2 Non-signature-based malware; Is this referring to malware that hasn't been identified and needs sandboxed?

Response: This is referring to malware that does not match known signatures. This malware could be identified through use of heuristics, behavior analysis, or threat intelligence feeds.

Question 11: Is the pricing in this section to be based on the 27,000 user number from item 11.3.2?

Response: The final number is unknown, but we are using the approximate number of state employees of 27,000 for a rough estimate. Vendor's proposing a flat fee should assume 27,000 users.

Question 12: Can pricing be tiered?

Response: Yes, the State will accept tiered pricing. Please see the Revised Cost Information Submission for a tiered-pricing option.

Question 13: 5.13 Any rates for services offered by the Vendors must not require a service term. Is this referring to the pricing submitted under Annual Costs in Section VIII? Does ITS want a 5 year price without a five year term (ie: (5) 1 year terms, or a month to month contract that is good for 5 years?)

Response: Evaluation will be performed based on a 5-year lifecycle cost. The initial term of the contract will be for 5 years and allow for up to two (2) additional two-year terms. Termination of the contract will be governed by Article 15 of Exhibit A.

Question 14: Is it MS ITS intent for Managed Services to include day-to-day analysts roles for investigation and triage of incidents, or should the Managed Service only include on-demand subject matter expertise to support the State's Help Desk with elevated cases?
a. If the State is opting for day-to-day analysts does the State require 24.7 coverage?
b. If the State is opting for day-to-day analysts what is the anticipated incident load?

Response: **Day-to-day analysts are not required, but the State is interested in seeing options for pricing for both day-to-day and on-demand options. There are no anticipated case load volumes. If a vendor would like to provide future cost associated with this activity, please provide that cost in the Optional Table in the Revised Cost Information Submission.**

Question 15: Is it MS ITAS intent for Managed Services to include management and remediation of daily help desk tickets, or should the Managed Service only include on-demand subject matter expertise to support the State's Help Desk with elevated cases?
a. If the State is opting for day-to-day help desk management does the State require 24.7 coverage?
b. If the State is opting for day-to-day help desk management what is the anticipated case load?

Response: **Please see the response to Question Number 14.**

Question 16: Is it MS ITS intention that all Agencies using the system will be Managed or will agencies have the option to be Managed or Non-Managed?

Response: **Agencies will have the option to utilize managed services based on their discretion pursuant to Section VII 11.2.2. ITS may choose to have the service managed at the Enterprise level pursuant to Section VII 11.2.1 for global administration.**

Question 17: Please check the services that MS ITS would consider as required (R) and like to have (L) in the Managed Services offering,
Version Upgrade Assurance
Application Patching
Operating System Patching
Policy Development
Policy Configuration
Policy Optimization
Incident Analysis
Incident Remediation
Critical Incidents Updates to Management
HR & Legal Review & Planning
End User Training
Administration Training
Administration Mentoring/Team Building
Agency Onboarding
Agency by Agency Optimization Planning Sessions
Weekly Reporting
Monthly Reporting
Quarterly Reporting

Response: **Managed Services Options:**
Version Upgrade Assurance - R
Application Patching - R
Operating System Patching - R
Policy Development - R

Policy Configuration - R
Policy Optimization - R
Incident Analysis - L
Incident Remediation – N/A
Critical Incidents Updates to Management - L
HR & Legal Review & Planning – N/A
End User Training - Section VII 13.3
Administration Training - Section VII 13.3
Administration Mentoring/Team Building - L
Agency Onboarding - Section VII 13.2.1
Agency by Agency Optimization Planning Sessions - Section VII 13.2.2
Weekly Reporting - R
Monthly Reporting - R
Quarterly Reporting - R

Question 18: Our solution is priced on a per user basis. Can you please indicate the number of users that we need to license? If this is not possible can you please indicate a minimum number of users to be quoted so that all suppliers can adequately size the scope of the service.

Response: **The final number of users is unknown, but we are using the approximate number of state employees of 27,000 for a rough estimate. Vendor's proposing a flat fee should assume 27,000 users.**

Question 19: Does the State of Mississippi and/or any of its agencies currently uses a CASB or SWG solution?

Response: **CASB and SWG are not in use at the enterprise level nor at any agency to ITS' knowledge.**

Question 20: Can you please provide a standard or a statement indicating the scope of the assessment described on item 5.14

Response: **The third-party security assessment should review and assess all aspects of the system and configuration including vendor/cloud hosted and on premises components. This should also include penetration testing to determine any existing vulnerabilities.**

Question 21: For the questions on paragraph 6.3 we would like to answer in terms of the qualifications and requirements for the individuals that will provide the support and service as opposed to an individual's name. Is this acceptable by the State of Mississippi

Response: **Yes, Vendor may redact names from resumes or only provide qualifications for individuals proposed.**

Question 22: We understand that requirements described in the item 11.6 requires the solution to operate independently for each of the agencies is this the case? Can you please describe how the users in the different agencies are separated? Do agencies have their own domain? Do agencies have their own Active Directory or Similar solution?

Response: **Currently, internal and external IP addresses are delineated at the agency level. From a user perspective, most agencies maintain an active directory that could be used for authentication. The solution should work with active directory as well as agencies that do not have a centralized directory. The State has an enterprise active directory that could be utilized if needed.**

Question 23: Can you please describe the requirements of item 12.3.1

Response: **See the response to Question #7 above**

Question 24: Can you please explain in more details the requirements of item 12.10

Response: **There have been instances in the past where agencies would use a standard port (i.e., 80 or 443) to mask other protocols/applications. The solution should be able to detect this so that a policy can be written to address this traffic.**

Question 25: How does the State of Mississippi plans to provide the "customer provided classification of websites" indicated in item 12.14

Response: **This should be configurable at either the enterprise or agency level. Classifications should be able to be entered manually through the portal or through a batch upload process.**

Question 26: We understand there are 27K employees along with contractors, What User Count we should build the proposal for?

Response: **The final number of users is unknown, but ITS is using the approximate number of state employees of 27,000 for a rough estimate of user counts.**

Question 27: For references, would you prefer the reference be for the Web Gateway, Managed Service Provider or both?

Response: **Vendor can provide both.**

Question 28: What is the allocated budget for this project?

Response: **State agencies budgets are available to be viewed at www.transparency.ms.gov.**

Question 29: Will each state agency's security posture be expected to be different or adhere to a single statewide security posture controlled by ITS?
a. If different, will ITS manage/control the security posture or will it be the individual agency?
b. If the same will ITS manage/control the security posture or will it be shared between ITS and the individual agency.

Response: **Each agency must adhere to the State's Enterprise Security Policy. ITS has legislative authority to set minimum standards at the enterprise level but agencies can implement more stringent controls, as long as those**

controls fit into the architecture of the enterprise network and do not negatively impact enterprise security controls. For this secure web gateway project, ITS will be responsible for management and oversight of the global administration and settings (Section VII 11.2.1). As such, ITS will set minimum levels at the global level that cannot be overridden by agencies (Section VII 11.5).

Question 30: Is the ability to write granular security policies around the user, device and application important to ITS?

Response: **Yes.**

Question 31: Will agency traffic within the Enterprise State Network be managed by ITS?

Response: **Yes.**

Question 32: For agencies supported within the Enterprise State Network, will there be any requirements for separate connectivity to the proposed solution outside of the referenced 5Gbps connection today? If so, can you provide bandwidth requirements for the separate connections? If so, would it be helpful to support any IPSEC VPN tunnel device in the separate remote or branch office service connections to the unified cloud gateway?

Response: **For connectivity to and from the Enterprise State Network, the existing 10 Gbps of internet connectivity will be used. This includes any separate remote/branch office connections.**

For state owned devices that are off the network, they should be protected just like they are on the network. We do not know remote connection bandwidths but anticipate it to be limited to consumer grade internet connections.

Question 33: Will there be any future use case requirement for SDWAN within this solution?

Response: **There are no current plans for SDWAN.**

Question 34: Within the zero trust framework of the solution, is there a requirement to create a more persistent secure inspection of data and users other than whitelisting?

Response: **This is not a requirement, but the State is interested in options that the responding vendors can provide. Section VII 12.12 lists requirements for detection and blocking for the Secure Web Gateway product.**

Question 35: Could we have samples of incident, problem and change tickets from the current solution that we could examine? That should include quantity totals over a period of time and specify how many users are representative (does it include for instance all 80 agencies)? This will allow for a more precise labor sizing.

Response: **The State does not have a current secure web gateway project so we cannot anticipate ticket volumes.**

Question 36: What is the expected amount of labor that would be provided by ITS vs by the vendor?

Response: **If ITS were to opt for the managed service option, then the vendor would be providing all labor. Regardless of the managed service offering, ITS plans to take trouble tickets and change requests from agencies through our NOC and work with the vendor directly.**

Question 37: Is trusted traffic flow such as backup data expected? Are backups done to a cloud provider or to an on-prem solution?

Response: **Both. Some agencies are utilizing public cloud providers for back up services today and some are utilizing the State's private cloud in our data center. ITS is currently examining options for public cloud connectivity and we expect to have private connectivity to some public clouds soon.**

Question 38: Is Remote Access VPN a requirement for the solution?

Response: **No, the State has an existing enterprise VPN solution.**

Question 39: What is the total number of agencies that will be using this service?

Response: **There are approximately 80 agencies that participate in the state network. (Section VII 11.3.1)**

Question 40: Should the solution be completed managed by 3rd party?

Response: **The State is interested in options for a managed service but utilization of these services will ultimately be a business decision. (Section VII 11.2)**

Question 41: Will the State need to maintain day to day management of other agencies?

Response: **For this secure web gateway project, ITS will be responsible for management and oversight of the global administration and settings (Section VII 11.2.1). As such, ITS will set minimum levels at the global level that cannot be overridden by agencies (Section VII 11.5). Agencies should have management functionality for all non-security settings along with reporting functionality. (Section VII 11.6)**

Question 42: What is ITS current infrastructure is comprised of, such as on-premises, and/or Hybrid environment such as AWS, Azure, GCP etc.?

Response: **There is no current secure web gateway in place at the enterprise level. Currently public cloud has limited adoption from a few agencies but ITS is actively examining options for public cloud connectivity. See Question #7 above for more detail on the current infrastructure.**

Question 43: For the Secure Web Gateway, is the State looking to secure (WAN, VPN, ZTNA) just for the Primary and DR site, or does it include remote locations as well?

Response: **Currently all network ingress and egress are from the two halves of the network core (Eastwood Data Center and Woolfolk Building). This includes traffic to/from the approximately 1100 remote sites on the State's MPLS WAN. Over the course of this contract, ITS anticipates changes to the current perimeter security border, which may change the current configuration. The awarded vendor's options for Section VII 11.8 could directly impact that.**

Question 44: Besides users, what services and applications must be protected by the proposed solution?

Response: **All outbound traffic should be inspected. The solution should not be strictly limited to HTTP and HTTPS, but also variations of those protocols; other protocols such as FTP, IM, and streaming media; and any other client-initiated traffic. Due to the ever-changing landscape of IT, long term plans could include public cloud instances sponsored by the State.**

Question 45: What is the type and number of services, workloads, storage, and applications running in the current environment?

Response: **Due to the decentralized nature of IT in Mississippi state government, we cannot feasibly provide accurate information.**

Question 46: Is ITS open to discuss services and applications hosted in the cloud / hybrid cloud solution?

Response: **The solution must be vendor and/or cloud hosted (Section VII 11.7)**

Question 47: Please clarify below excerpt from section 3.1 about the security of the site. Is it for infrastructure security only, or does it include physical security? Please also clarify how ITS currently managing the data centers.

E. Providing security for the site that is agreeable to ITS with Licensor responsible for all necessary equipment and software related to security;
F. Maintaining the accessibility of the site twenty-four (24) hours a day, seven (7) days a week at an uptime rate of 99.9% or greater, subject to the limitations set forth in this Agreement, including but not limited to, those in Article 4.4;
G. Completing daily backups of the site;
H. Notifying ITS at least three (3) business days prior to any anticipated service interruption, with said notice containing a general description of the reason for the service interruption;

Response: **The State assumes the vendor is referring to Article 3.2 of the Standard Contract. This article is referring to security of the service offering itself. Since this is to be a vendor/cloud hosted solution, the vendor or cloud provider would be responsible for physical security in the hosting environment. ITS is responsible for physical security for any on-premises equipment installed in our data center.**

E. "Site" in this instance refers to the Secure Web Gateway product itself.
F. This refers to both the management portal that will be used to manage the service by ITS and the agencies, as well as the service itself.

G. Vendor must perform daily backup of configurations for the State's Secure Web Gateway configuration.
H. The Exhibit A, Standard Contract is being modified. See Amendment Number 4 above.

Question 52: To meet the SLAs such as site 24/7 availability, workload and data protection, Is ITS looking for a Co-located facility for both the DC and DR?

Response: **The solution must be vendor and/or cloud hosted (Section VII 11.7)**

Question 53: Section VII sections 3, 11.2, 11.3 and 11.4 seem to conflict. Can the State provide guidance on the sort of ongoing management services it is requesting? Can you describe in more detail the request for the ongoing management services?

Response: **Ideally ITS will have sufficient staff with cycles to manage the solution at the enterprise level. ITS will administer global settings (Section VII 11.5), work with agencies on issues, and provide general support for the platform. However, based on workload and work force, ITS may wish to turn over day-to-day management to the vendor and pay the vendor to provide that function. (Section VII 11.2.1). For any configuration options that an agency may have, they may choose to utilize a managed service. (Section VII 11.2.2)**
Regardless of the managed service offering, ITS plans to take trouble tickets and change requests from agencies through our NOC and work with the vendor directly.
Section VII 11.4 means that other entities besides ITS may utilize this RFP to procure services. These entities could be schools, libraries, community colleges, universities, or local governing authorities. If any of these other entities were to use these services, then ITS would not be involved in management. These other entities may choose to use the proposed managed services as needed.

Question 54: What are the State's expectations of the vendor and what management capabilities would you like to have in the system for state agencies and their personnel? Vendor options: Monitoring, Incident/Problem Management, Capacity Mgt., Dedicated Customer Success Manager, etc.? State Options: Move Add & Changes, Configuration, Patch Management, Report access, etc.?

Response: **See also the response to Question 17.**
Required regardless of Managed Services or not:

- **Capacity Mgt. (Required per Section VII 12.8.1)**
- **Dedicated Customer Success Manager (Required per Section VII 13.1.4.1)**

Vendors should detail their base service offering and what options would be considered part of their managed service offering.

Question 55: ITS RFP Response Checklist: ITS is requesting a labeled USB with vendor name and RFP number. Do you mean for this label to be electronic, physically on the outside of the thumb drive, or can the thumb drive be submitted in a sealed envelope with this requested label on the outside?

Response: **It is preferred that the USB be labeled with the vendor's name. It is required for the USB to be submitted in a sealed envelope/package with the information from the cover page clearly affixed to the package. See Proposal Submission Requirements, Section II.**

Question 56: If responses to vendor submitted questions are not supplied by the date specified in the RFP, would the State be open to extend the due date?

Response: **Yes, please see the revised Procurement Project Schedule above.**

Question 57: In regards to technical specification 12.2 (Users' traffic from the Enterprise State Network must present to the Internet as State-owned IP addresses over the State Data Center's Internet circuits),

Can the State estimate the percentage of this traffic that must be presented as State-owned IP Address?

Does this include traffic originated from an employee work-at-home or other remote locations?

Response: **Traffic leaving the State's firewall will be state-owned IPs. The State has additional IPs that we could assign to the SWG solution or would be willing to entertain a X-Forwarded-For option. If the State chooses to present traffic from the SWG solution using State-owned IP addresses, then 100% of that traffic should be State-owned IPs. Regardless of the solution chosen, the State is interested in receiving Netflow/IPFIX data from the SWG solution.**

No, it does not include traffic originating from work-at-home or other non-State remote locations. For State owned devices that are off the network, they should be protected just like they are on the network.

Question 58: In regards to technical specification 13.5 (Support)

Can the State confirm that ITS will be that will be taking the initial call from end-users (tier 1) to triage and/or confirm the vendor will need to be engaged?

Response: **For the ITS/State Network implementation of the service, yes, ITS plans to take trouble tickets and change requests from agencies through our NOC and work with the vendor directly. Tier 1 user support occurs at the agency level and they will engage ITS to enter a ticket with the secure web gateway vendor when necessary.**

For other entities utilizing this RFP (Section VII 11.4), those entities will be responsible for Tier 1 support.

Question 59: How many employees will be supported with the initial purchase?

Response: **The final number of users is unknown, but we are using the approximate number of state employees of 27,000 for a rough estimate.**

Question 60: What does the roll out look like as far as users as this project progresses: 6-months, 12-months, 18-months, …etc?

Response: **This will ultimately depend on the migration plan that is agreed upon by ITS and the vendor. ITS wants to roll this out as soon as possible, but the speed of this migration will depend on the complexity of the deployment and availability of the agencies.**

Question 61: Initially, how many employees will need to be trained

Response: **For ITS at the enterprise level, there will need to be approximately 6 users trained. As agencies are brought on board, their administrators and IT staff will need to be trained. ITS expect that the migration will occur in phases so training will correspond to agencies being onboarded to the solution. Vendors should either propose training as a per person unit cost or a flat fee for unlimited training sessions.**

Question 62: Would you like to include service hours to familiarize your team with the solution?

Response: **No, Vendors should provide training hours and associated costs as detailed in Section VII Item 13.3.**

Question 63: Do you need an instance for testing?

Response: **The state is open to this idea and would like details and pricing on how this could occur. At this point, we do not have an anticipated case load volume. If a vendor would like to provide future costs associated with this activity, please provide that cost in the Optional Table in the Revised Cost Information Submission.**

Question 64: Will the State provide high-level diagrams of State's existing architecture? (Section 12.1.1, 12.3.1)?

Response: **See the response to Question #7 above.**

Question 65: The solution should not be strictly limited to HTTP and HTTPS, but also variations of those protocols; other protocols such as FTP, IM, and streaming media; and any other client-initiated traffic

1. "other protocols such as FTP, IM and streaming media". Does this indicate the requirements to support internet defense on all out-bound ports or only on Secure Web Gateway ports of 80/443?

Response: **All outbound traffic should be inspected. Most of this traffic is expected to be HTTP and HTTPS.**

Question 66: Section 12.2: Users' traffic from the Enterprise State Network must present to the Internet as State-owned IP addresses over the State Data Center's Internet circuits.

1. Does this indicate that private user attribution information (including State-IP addresses) at a minimum be presented to the ITS as part of monitoring and logging?
2. If so, does this indicate that bulk IP-addresses owned by the vendor (that are shared with the state) for cloud-based deployments can be used to logically

separate, encrypt, protect privacy, optimize performance, bandwidth and latency end-to-end of the overall Secure Web Gateway solution as required in Section 11.4, 11.6, 12.8, 12.11, or 16.4.1?

Response: **Traffic leaving the State's firewall will be state-owned IP's. Each agency is assigned a small block of public IPs for NAT/PAT. From a monitoring/logging perspective, the State will need to be able to cross-reference these public IPs to outbound IPs from the SWG solution.**

We have additional IP's that we could assign to the SWG solution or would be willing to entertain a X-Forwarded-For option. If the State chooses to present traffic from the SWG solution using State-owned IP addresses, then 100% of that traffic should be State-owned IPs. Regardless of the solution chosen, the State is interested in receiving Netflow/IPFIX data from the SWG solution.

RFP responses are due May 26, 2022, at 3:00 p.m. (Central Time).

If you have any questions concerning the information above or if we can be of further assistance, please contact Bill Brinkley at 601-432-8241 or via email at Bill.Brinkley@its.ms.gov.

Attachment: Attachment A: Revised Cost Information Submission

cc: ITS Project File Number 44639